Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2512

Vragen van de leden **Verhoeven** en **Pia Dijkstra** (beiden D66) aan de Ministers van Volksgezondheid, Welzijn en Sport en van Veiligheid en Justitie over *het bericht «Noodtoestand in Amerikaans ziekenhuis wegens ransomware» (een chantagemethode op internet)* (ingezonden 30 maart 2016).

Antwoord van Minister **Schippers** (Volksgezondheid, Welzijn en Sport), mede namens de Staatssecretaris van Veiligheid en Justitie (ontvangen 12 mei 2016).

Vraag 1
Kent u het bericht «Noodtoestand in Amerikaans ziekenhuis wegens ransomware»?[1]

Antwoord 1
Ja.

Vraag 2, 3
Is een dergelijke situatie reeds in Nederland voorgekomen? Kunt u dit uitsluiten? Zo nee, waarom niet?
Deelt u de mening dat deze situatie ook in Nederlandse ziekenhuizen mogelijk is? Zo nee, waarom niet?

Antwoord 2, 3
Een dergelijke situatie in de vorm van een noodtoestand binnen de Nederlandse gezondheidszorg is mij niet bekend. Het Nationaal Cyber Security Centrum (NCSC) is bekend met signalen dat in Nederland, ziekenhuizen, evenals andere sectoren, geconfronteerd worden met aanvallen op kantoorautomatisering door ransomware. Bij het NCSC zijn echter geen signalen bekend dat deze aanvallen hebben geresulteerd in grootschalige uitval of verstoring.
Melding van dit type incidenten bij de Autoriteit Persoonsgegevens (AP) is wettelijk verplicht indien er persoonsgegevens gecompromitteerd zijn. Per 1 januari 2016 geldt immers de wettelijke meldplicht datalekken. De Autoriteit Persoonsgegevens heeft beleidsregels over deze meldplicht opgesteld[2]. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er

[1] https://www.security.nl/posting/465461/Noodtoestand+in+Amerikaans+ziekenhuis+wegens+ransomware
[2] https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

ah-tk-20152016-2512
ISSN 0921 - 7398
's-Gravenhage 2016

sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen. Of bij ransomware een datalek moet worden gemeld, hangt af van de ernst van het datalek. In het geval van ransomware moet de verantwoordelijke organisatie deze afweging niet beperken tot de gegevens op het gecompromitteerde apparaat. Hij moet het risico meewegen ten aanzien van alle soorten persoonsgegevens waarvan aangenomen kan worden dat die vanaf het randapparaat via een netwerkverbinding benaderd kunnen worden.
De IGZ heeft op 17 maart 2016 de brancheorganisaties Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU), Zelfstandige Klinieken Nederland (ZKN), GGZ Nederland en Revalidatie Nederland (RN) en hun leden per brief gewezen op de meldplicht datalekken[3]. Daarbij heeft de IGZ de koepels en hun leden ook opgeroepen een dergelijk incident vrijwillig te melden aan de IGZ.

Vraag 4, 5
Kunt u aangeven wat voor voorzorgsmaatregelen er worden genomen om dergelijke situaties te voorkomen?
Zijn er bepaalde richtlijnen, bijvoorbeeld vanuit het Nationaal Cyber Security Centrum, met betrekking tot de inrichting van ICT-systemen van Nederlandse ziekenhuizen om data van patiënten te beschermen? Zo ja, kunt u aangeven welke richtlijnen dit zijn?

Antwoord 4, 5
Informatiebeveiliging is een eigen verantwoordelijkheid van ziekenhuis. Vanuit de sectorale verantwoordelijkheid voor de zorg bestaat thans reeds een uitvoerig wettelijk kader ter bescherming van gegevens.
De eisen voor informatiebeveiliging voor ziekenhuizen zijn te vinden in de NEN 7510[4], NEN 7512 en NEN 7513 voor respectievelijk veilige omgang met informatie, gegevensuitwisseling en het vastleggen van acties op elektronische patiëntdossiers. IGZ gebruikt deze normen om te toetsen of ziekenhuizen qua informatiebeveiliging voldoende maatregelen hebben genomen om de continuïteit en kwaliteit van zorg te kunnen waarborgen. In een algemene maatregel van bestuur (AMvB) behorend bij het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens, dat ter behandeling voorligt in de Eerste Kamer, worden op grond van artikel 26 Wet bescherming persoonsgegevens (Wbp) specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling en zorginformatiesystemen wettelijk verankerd door het voldoen aan de bovengenoemde NEN-normen verplicht te stellen.
In de komende periode zal daarnaast de Netwerk- en InformatieBeveilingsrichtlijn (NIB-richtlijn), waarover eind 2015 binnen de EU een politiek akkoord bereikt is, worden geïmplementeerd. Hierin is de zorg ook genoemd. Deze NIB-richtlijn bestaat onder andere uit een zorg- en meldplicht. Uw Kamer wordt door het Ministerie van Veiligheid en Justitie reeds periodiek geïnformeerd over de voortgang van de NIB-richtlijn.
Daarnaast publiceert ook NCSC richtlijnen met betrekking tot de inrichting en beveiliging van ICT-systemen. Deze kunnen tevens worden gebruikt als handvat bij de implementatie van beveiligingsvereisten. Ook publiceert het NCSC algemene whitepapers, factsheets en best practices en dagelijks adviezen over nieuwe kwetsbaarheden in hard- en software die voor een ieder, ook buiten de doelgroep van rijksoverheid en de vitale infrastructuur, te vinden zijn via de website www.ncsc.nl.
In aanvulling hierop bestaat een door het NCSC in samenwerking met de sector opgezet Information Sharing and Analysis Centre (ISAC) voor de zorg. Een ISAC is een publiek-private sectoraal samenwerkingsverband, waarbinnen op tactisch niveau deelnemers van verschillende ziekenhuizen onderling

[3] http://www.ggz-connect.nl/bericht/5619/igz-vraagt-aandacht-voor-informatiebeveiliging/document/downloaden/2750/brief%2BIGZ.pdf
[4] De norm NEN 7510 is een door het Nederlands Normalisatie-instituut ontwikkelde norm voor Informatiebeveiliging. De norm is gebaseerd op de Code voor Informatiebeveiliging. Dit de Nederlandse versie van de British Standards 7799, die later als internationale standaard voor informatiebeveiliging in organisaties is gepubliceerd. De Code voor Informatiebeveiliging bestaat uit twee delen: een norm (NEN-ISO/IEC 27001:2013+C11/2014 nl) en een «code of practice» (NEN-ISO/IEC 27002:2013+C2:2015 nl).

(incident) informatie en ervaringen uitwisselen over cybersecurity en kwetsbaarheden in de sector («situational awareness»). Door het delen van (incident) informatie en het opbouwen van een netwerk kunnen ziekenhuizen hun eigen informatiebeveiliging verbeteren.
Tot slot werken de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU) en GGZ Nederland, zoals ik in eerdere Kamervragen al aangaf, samen om in samenspraak met het NCSC, als verantwoordelijk Computer Emergency Response Team (CERT) voor de rijksoverheid en de vitale infrastructuur specifiek, een CERT voor de zorg (Z-CERT) in te richten.

Vraag 6
Krijgen artsen en medewerkers in ziekenhuizen «cyberhygiëne»-training om dergelijke infecties van ransomware (of malware) te voorkomen? Zo nee, waarom niet? Deelt u de mening dat het wenselijk is als hier wel voor gekozen wordt om mogelijke risico's te verminderen?

Antwoord 6
Borgen van continuïteit van dossiers is een verplichting van zorgaanbieders. Als zodanig is cyber-awareness daarvan een onderdeel. Het is de verantwoordelijkheid van de instellingen om zijn personeel op te leiden in het (veilig) omgaan met software. Het geven van trainingen kan daar, naast bijvoorbeeld het treffen van technische maatregelen, deel van uitmaken. Door ziekenhuizen is de afgelopen jaren dan ook actief geparticipeerd binnen de landelijke awareness-campagne Alert Online.

Vraag 7
Bent u bereid de ICT-systemen van Nederlandse ziekenhuizen te laten testen op het gebied van cybersecurity? Zo nee, waarom niet?

Antwoord 7
Zoals eerdere reeds aangegeven is het de eigen verantwoordelijkheid van ziekenhuizen om de informatiebeveiliging op orde te hebben. Ziekenhuizen kunnen hun informatiebeveiligheidsbeleid en de beveiligingsmaatregelen periodiek laten auditen. De NEN 7510 heeft aan deze periodieke toetsing een specifiek hoofdstuk gewijd. Sinds februari 2016 kunnen zorginstellingen zich ook laten accrediteren in het kader van NEN 7510 en zich laten certificeren door een onafhankelijke accrediterende partij. De IGZ neemt, wanneer zij kijkt naar de informatiebeveiliging, de uitkomsten en inzet van dergelijke toetsing mee in haar oordeel over hoe de instelling met informatiebeveiliging omgaat.